UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

KEITH TESKY, MARK TESSMER, CHRISTOPHER VANGOETHEM, KAL TESKY, on behalf of themselves and all others similarly situated**,**

Plaintiffs,

v.

BONE & JOINT CLINIC, S.C.,

Defendant.

Case No. 23-cv-184 - Consolidated

DEMAND FOR JURY TRIAL

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

Plaintiffs Keith Tesky, Mark Tessmer, Kenneth VanGoethem, and Kal Tesky ("Plaintiffs") bring this Consolidated Class Action Complaint against Bone & Joint Clinic, S.C. ("Bone & Joint" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations and facts of public record, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of Defendant Bone & Joint's failures to properly secure, safeguard, and adequately destroy Plaintiffs' and Class Members' sensitive personal identifiable information that it had acquired and stored for its business purposes.

2. Defendant's data security failures allowed a targeted cyberattack in January 2023 to compromise Defendant's network (the "Data Breach") that contained personally identifiable information ("PII") and protected health information ("PHI") (collectively, "the Private Information") of Plaintiffs and other individuals ("the Class").

3. Defendant Bone & Joint Clinic is a network of clinics with teams of orthopedic, pain management, and physical therapy experts located in Northcentral Wisconsin.

4. According to notices sent to the Department of Health and Human Services Office for Civil Rights ("HHS") and State Attorneys General, this Data Breach occurred on or about January 16, 2023, and included the Private Information of approximately **105,094** individuals, including Plaintiffs and Class.

5. Defendant launched an investigation into the Data Breach and confirmed that an unauthorized actor accessed its system on January 16, 2023 and may have copied and exfiltrated certain files containing Plaintiffs' and Class Members' Private Information.

6. Despite learning of the Data Breach on or about January 16, 2023 and determining that Private Information was involved in the breach on January 27, 2023, Defendant did not begin sending notices of the Data Breach (the "Notice of Data Breach Letter") until March 7, 2023.[1]

7. The Notice of Data Security Incident sent to Plaintiff states the following:

> **What Happened?** On January 16, 2023, Bone & Joint experienced a network disruption and immediately initiated an investigation of the matter and engaged cybersecurity experts to assist with the process. The investigation determined that certain administrative and medical files may have been acquired without authorization. After a thorough review of those files, on or about January 27, 2023, some of your personal information was identified as being contained within the potentially affected data.[2]

8. Based on the Notice of Data Breach Letter, Defendant admits that Plaintiffs' and Class Members' Private Information was unlawfully accessed and may have been exfiltrated by a third party.

9. The Private Information compromised in the Data Breach included certain personal or protected health information of current and former employees, patients and other individuals whose Private Information was maintained by Bone & Joint, including Plaintiffs.

10. Based on the public statements of Defendant to-date, a wide variety of PII and PHI was implicated in the breach. For patients, the breached information includes: name, date of birth, Social Security number, driver's license, home address, phone number, health insurance

[1] *See* Notice Letters, collectively attached as Exhibit A.

[2] *Id.*

information, diagnosis and treatment information; for employees, the breached information includes name, address, phone number, date of birth, Social Security number and other PII, which might include drivers' license number, State ID number and/or passport number. Similarly, employees' spouses, dependents and beneficiaries' PII was also exposed.[3]

11. The Private Information compromised in what Bone & Joint refers to as a "data security incident" happened when it "experienced a network disruption."[4] In other words, cybercriminals intentionally targeted Bone & Joint for the highly sensitive Private Information it stores on its computer network, attacked the insufficiently secured network, then exfiltrated highly sensitive PII and PHI, including but not limited to Social Security numbers – the gold standard for identity thieves, and PHI. As a result, the Private Information of Plaintiffs and Class remains in the hands of those cyber-criminals.

12. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for either treatment or employment or both.

13. Upon information and belief, it was common knowledge among employees that the Defendant and its CEO opted not to fix known vulnerabilities in their computer systems due to the perceived expense. Instead, Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Bone & Joint's computer network in a condition vulnerable to cyberattacks.

14. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to

[3] https://bonejoint.net/notice-of-data-security-incident/ (last visited May 8, 2023).

[4] *See* Ex. A.

Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

15. Upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendants' inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

16. Defendant through its privacy policy, both expressly and impliedly understood its obligations and promised to safeguard Plaintiffs' and Class Members' Private Information. Plaintiffs and Class Members relied on these express and implied promises when seeking out and paying for Defendant's services and agreeing to employment with Defendant for themselves and family members. But for this mutual understanding, Plaintiffs and Class Members would not have provided Defendant with their Private Information. Defendant, however, did not meet these reasonable expectations, causing Plaintiffs and Class Members to suffer injury.

17. Defendant disregarded the rights of Plaintiffs and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions;

failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff(s) and Class Members with prompt and full notice of the Data Breach.

18. In addition, Bone & Joint failed to properly monitor the computer network and systems that housed the Private Information. Had Bone & Joint properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals almost a month of unimpeded access to the PII and PHI of Plaintiffs and Class Members.[5]

19. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Bone & Joint collected and maintained is now in the hands of data thieves.

20. As a result of the Data Breach, Plaintiffs and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiffs and Class Members must now and for years into the future closely monitor their medical and financial accounts to guard against identity theft. As a result of Defendant's unreasonable and inadequate data security practices, Plaintiffs and Class Members have suffered numerous actual and concrete injuries and damages.

21. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiffs' and Class Members' Private Information was targeted, accessed, has been misused, and disseminated on the Dark Web.

22. As Defendant instructed, advised, and warned in its post Data Breach Notice Letter discussed below, Plaintiffs and Class Members must now closely monitor their financial accounts

[5] *See* https://www.prnewswire.com/news-releases/bone--joint-clinic-sc---notice-of-data-security-incident-301769464.html (last visited May 8, 2023).

to guard against future identity theft and fraud. Plaintiffs and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included, and will continue to include in the future: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

23. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (g) deprivation of value of their PII; and (h) the continued risk to their Sensitive Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it collected and maintained.

24. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach (the "Class").

25. Accordingly, Plaintiffs brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, (iv) breach of fiduciary duty; (v) invasion of privacy, (vi) unfair and deceptive

practices, (vii) confidentiality of patient records, (vii) unjust enrichment, and (ix) declaratory and injunctive relief.

26. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

27. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiffs' and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

PARTIES

28. Plaintiff Keith Tesky is an adult individual who at all relevant times has been a citizen and resident of the State of Wisconsin. He was a patient of Bone & Joint. Plaintiff Tesky received notice of the Data Breach dated March 7, 2023. *See* Ex. A.

29. Plaintiff Mark Tessmer is an adult individual who at all relevant times has been a citizen and resident of the State of Wisconsin. Plaintiff's PHI and PII records were maintained within Defendant's networks, as Plaintiff is both a former employee and a former patient of Defendant's. Plaintiff Tessmer received notice of the Data Breach dated March 7, 2023. Ex. A.

30. Plaintiff Christopher VanGoethem is an adult individual who at all relevant times has been a citizen and resident of the State of Wisconsin. He resides in Wausau, Wisconsin where he intends to remain. He received notice of the Data Breach dated March 7, 2023. *See* Ex. A.

31. Plaintiff Kal Tesky is a Citizen of Wisconsin residing in Lincoln County, Wisconsin. Plaintiff received a letter dated March 7, 2023, from Defendant Bone & Joint notifying

Plaintiff that Defendant's network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

32. Defendant Bone & Joint Clinic, S.C. ("Defendant") brands itself as an independent, comprehensive team of orthopedic, pain management, and physical therapy experts. https://bonejoint.net/why-bone-joint/ (last visited 5/8/2023). Bone & Joint is a Wisconsin Service Corporation organized under the laws of Wisconsin, and its principal place of business is located at 225000 Hummingbird Rd, Ste. 100, Wausau, Wisconsin 54401.

JURISDICTION AND VENUE

33. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, some of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

34. This Court has personal jurisdiction over Defendant because it is a Wisconsin service corporation that operates and is headquartered in this District and conducts substantial business in this District.

35. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

Defendant's Business and Collection and Storage of Private Information

36. Defendant Bone & Joint has been providing health services since 1969. It provides "care for degenerative diseases like arthritis, sports injuries, fractures, sprains, ligament tears, structural abnormalities, sciatica, herniated disc, degenerative disc disease, and many other types of orthopedic conditions." *See* https://bonejoint.net/faqs/ (last visited May 10, 2023). Defendant advertises its use of "cutting edge technology" like "the most current digital X-ray technology" and the "Mako Robotic-Arm" for joint replacement procedures.[6]

37. Bone & Joint has 7 locations where "a team of 28 providers offer[s] multispecialty orthopedic care at four clinic locations and 12 therapists provid[e] physical and occupational therapy at three therapy locations throughout Central Wisconsin." *Id.*

38. For the purposes of this Class Action Complaint, all of Bone & Joint's associated locations will be referred to collectively as "Bone & Joint."

39. In the ordinary course of business, including employment services and receiving medical care services from Bone & Joint, each patient and employee must provide, and Plaintiffs did provide, Bone & Joint with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;
- Marital status;
- Employer with contact information;

[6] *See Why Bone & Joint?*, BONE & JOINT, https://bonejoint.net/why-bone-joint/ (last visited May 20, 2023).

- Primary and secondary insurance policy holders' name, address, date of birth, and Social Security number;
- Demographic information;
- Driver's license or state or federal identification;
- Information relating to the individual's medical and medical history;
- Insurance information and coverage; and
- Banking and/or credit card information.

40. Defendant also creates and stores medical records and other protected health information for its patients, including records of treatments and diagnoses.

41. Upon information and belief, Bone & Joint's HIPAA Privacy Policy is provided or made available to every patient both prior to receiving treatment, and upon request.

42. Bone & Joint agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA"). Under state and federal law, businesses like Defendant have duties to protect current and former patients' PII/PHI and to notify them about breaches.

43. Defendant recognizes these duties, declaring that:

a. "Bone & Joint has a commitment to promote adherence to applicable federal, state, and local laws and regulations as they relate to the provision of health care services."[7]

[7] *Our Commitment to Compliance*, BONE & JOINT, https://bonejoint.net/compliance-hotline/ (last visited May 20, 2023).

b. "At Bone & Joint Clinic, S.C., we take the privacy and security of personal information very seriously."[8]

44. Via its Privacy Policy, Defendant reaffirms—and advertises—its duties to protect patient PII/PHI. Specifically, Defendant declares:

a. "Bone and Joint Clinic is required to [maintain] the privacy of your health information," and

b. "Bone and Joint Clinic will not use or disclose your health information without your authorization."[9]

45. Yet, through its failure to properly secure the Private Information of Plaintiffs and Class, Bone & Joint has not adhered to its own promises of employee and patient rights.

46. The Private Information held by Bone & Joint in its computer system and network included the highly sensitive Private Information of Plaintiffs and Class Members.

The Data Breach

47. A data breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Bone & Joint.

48. On or about January 16, 2023, Defendant discovered its network had been breached via cyberattack.

49. Following a forensic investigation, Defendant then discovered that unknown

---

[8] *Notice of Data Breach*, MAINE ATTY GEN. (Mar. 7, 2023) https://apps.web.maine.gov/online/aeviewer/ME/40/29fd2d6e-2fed-4849-addf-0520e1562f7b.shtml.

[9] *Notice of Privacy Practice*, BONE & JOINT, https://bonejoint.net/wp-content/uploads/2022/09/Notice-of-Privacy-Practices-BJC.pdf,[archived at https://web.archive.org/web/20220930161457/https://bonejoint.net/wp-content/uploads/2022/09/Notice-of-Privacy-Practices-BJC.pdf] (last visited Mar. 21, 2023).

cybercriminals had accessed, obtained, and exfiltrated the Private Information of approximately **105,094 individuals** were affected.[10]

50. Defendant Bone & Joint's Notice of Data Breach admits that Plaintiffs' and Class Members' Private Information was accessed without authorization.[11]

51. Defendant further admits that cybercriminals not only viewed and accessed Plaintiffs' and Class Members' Private Information, but also acquired it from Defendant's network, meaning the Private Information was exfiltrated.[12]

52. Defendant had obligations created by HIPAA, FTCA, contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

53. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

54. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Bone & Joint, are well-aware of the risk of being targeted by cybercriminals.

55. Individuals place a high value not only on their PII, but also on the privacy of that

[10] Breach Portal, U.S. Dept. of Health and Hum. Servs., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited May 8, 2023).

[11] Notice of Data Security Incident, Bone & Joint, https://bonejoint.net/notice-of-data-security-incident/ (last visited May 8, 2023).

[12] *Id.*

data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

56. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[13]

57. Individuals, like Plaintiffs and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

58. Data breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

59. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will

[13] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited May 10, 2023).

have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[14]

60. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[15]

61. Additionally, in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[16]

62. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

63. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[17] This publication also explains that "[t]he FBI does

[14] https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 10, 2023).

[15] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last visited May 10, 2023).

[16] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last visited May 10, 2023).

[17] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last visited May 10, 2023).

not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[18]

64. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

Data Breaches are Rampant in Healthcare.

65. Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

66. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[19]

67. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily

[18] *Id.*

[19] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited May 10, 2023).

monetized."[20]

68. The HIPAA Journal article goes on to explain that patient records, like those stolen from Bone & Joint, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[21]

69. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[22]

70. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[23]

71. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[24]

---

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] https://www.ahu.edu/blog/data-security-in-healthcare (last visited May 12, 2023).

[24] *9 Reasons why Healthcare is the Biggest Target for Cyberattacks*, Swivelsecure, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited May 20, 2023).

72. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

73. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[25] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about one dollar.[26]

74. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers,

[25] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[26] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

> having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[27]

75. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can sell for up to $1,000 online."[28]

76. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

Defendant Failed to Properly Protect Plaintiffs' and Class Members' Private Information

77. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

78. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

---

[27] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[28] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

79. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

80. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[29]

81. To prevent and detect unauthorized cyber-attacks, as recommended by the United States Government, Defendant could and should have proactively taken the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

[29] *See generally Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business*, FED. TRADE COMM., https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last visited May 1, 2023).

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[30]

82. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.

[30] *Id.* at 3-4.

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it.

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[31]

83. To prevent and detect cyber-attacks, as recommended by the Microsoft Threat Protection Intelligence Team, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

[31] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Aug. 23, 2021).

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[32]

84. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiffs and Class Members.

85. As a result of computer systems in need of security upgrades, inadequate

[32] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited May 12, 2023).

procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

86. Because Defendant failed to properly protect and safeguard Plaintiffs' and Class Members' Private Information, an unauthorized third party was able to access Defendant's network, and access Defendant's database and system configuration files and exfiltrate that data.

Value of PII and PHI

87. The PII and PHI of consumers remains of high value to criminals, as evidenced by the prices offered through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[33] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[34] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[35]

88. Based on the foregoing, the information compromised in the Data Breach is

---

[33] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[34] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, available at: https://www.privacyaffairs.com/dark-web-price-index-2021/.

[35] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

89. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information…[is] worth more than 10x on the black market."[36]

90. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

91. There is also a robust legitimate market for the type of sensitive information at issue here. Marketing firms utilize personal information to target potential customers, and an entire economy exists related to the value of personal data.

92. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[37]

93. As such, future monitoring of financial and personal records is reasonable and necessary well beyond the one of protection offered by Defendant.

---

[36] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[37] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Aug. 23, 2021).

Defendant's Violations

Defendant Failed to Comply with FTC Guidelines

94. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

95. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[38]

96. The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

97. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

98. Furthermore, the FTC explains that companies must:

[38] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

99. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

100. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

101. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions clarify the measures businesses take to meet their data security obligations.

102. Defendant failed to properly implement basic data security practices.

103. Defendant's failure to employ reasonable and appropriate measures to protect

against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Defendant Failed to Comply with Industry Standards

104. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

105. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendant, including, but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

106. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

107. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

108. The foregoing frameworks are existing and applicable industry standards in the

healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

109. Upon information and belief, Defendant failed to comply with one or more of the foregoing industry standards.

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

110. HIPAA requires covered entities and business associates of covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

111. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

112. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

113. A data breach such as the one Defendant experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI that is not permitted under HIPAA.

114. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

115. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[39]

116. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

[39] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4.

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

117. Accordingly, Defendant's Data Breach resulted from a combination of insufficiencies that demonstrates Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant's Negligent Acts and Breaches

118. Defendant participated and controlled the development, implementation and enforcement of its privacy policy and controlled the process of gathering the Private Information from Plaintiffs and Class Members.

119. Defendant therefore assumed and otherwise owed duties and obligations to Plaintiffs and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, testing of the data security policies and network systems. Defendant breached these obligations to Plaintiffs and Class Members and/or were otherwise negligent because they failed to properly implement data security systems and policies for its health providers network that would adequately safeguarded Plaintiffs' and Class Members' Private Information. Upon information and belief, Defendant's unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

a. Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiff's and Class Members Private Information;
b. Failing to properly monitor its data security systems for data security vulnerabilities and risk;
c. Failing to test and assess the adequacy of its data security system;
d. Failing to develop adequate training programs related to the proper handling of emails and email security practices;
e. Failing to put into develop and place uniform procedures and data security protections for its healthcare network;
f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;
g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic

process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

p. Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

q. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

r. Failing to implement or update antivirus and malware protection software in need of security updating;

s. Failing to require encryption or adequate encryption on its data systems; and

t. Otherwise negligently and unlawfully failing to safeguard Plaintiff's and Class Members' Private Information provided to Defendants, which in turn allowed cyberthieves to access its IT systems.

Named Plaintiffs' Experiences

Plaintiff Keith Tesky

120. Plaintiff Keith Tesky is and at all times mentioned herein was an individual citizen residing in the State of Wisconsin.

121. Keith Tesky is and was a patient of Bone & Joint for over 20 years at all times relevant to this Complaint.

122. He received a Notice of Data Breach Letter related to Bone & Joint's Data Breach that is dated March 7, 2023. *See* Exhibit A.

123. The Notice Letter does not explain exactly which parts of his PII and PHI were accessed and taken but instead generically states that the files contained his "name, date of birth,

Social Security number, home address, phone number, health insurance information, and diagnosis and treatment information." *See* Ex. A.

124. He is especially alarmed by the vagueness of his stolen Private Information and that his Social Security number was identified as among the breached data on Bone & Joint's computer system.

125. Since the Data Breach, he monitors his financial accounts diligently, spending more time than he spent prior to learning of the Bone & Joint's Data Breach.

126. He is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Bone & Joint's Data Breach.

127. Starting in approximately in January 2023, he began receiving an excessive number of spam calls and texts on the same cell phone number used at Bone & Joint. These calls are a distraction, must be deleted, and waste time each day. This was not typical before the Data Breach. Given the timing of the Data Breach, he believes that the calls are related to his stolen PII.

128. In addition, he has received notifications and messages for McAfee that his information has been found on the Dark Web since the data breach occurred.

129. He suffered actual injury from the exposure and theft of his Private Information.

130. He has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession—is protected and safeguarded from additional breaches.

131. Had he been aware that Bone & Joint's computer systems were not secure, he would not have entrusted Bone & Joint with his PII and PHI.

Plaintiff Mark Tessmer

132. Plaintiff Mark Tessmer is and at all times mentioned herein was an individual citizen residing in the State of Wisconsin.

133. Plaintiff is both a former employee and a former patient of Defendant's. Plaintiff's PHI and PII records were maintained within Defendant's networks.

134. He received a Notice of Data Breach Letter related to Bone & Joint's Data Breach that is dated March 7, 2023. *See* Exhibit A.

135. The Notice Letter references his Private Information stored and maintained both a former employee and a former patient but does not explain exactly which parts of his PII and PHI were accessed and taken." *See* Ex. A.

136. He is especially concerned that his Private Information was stolen and that his Social Security number was identified as among the breached data on Bone & Joint's computer system.

137. Since the Data Breach, he monitors his financial accounts diligently, spending more time than he spent prior to learning of the Bone & Joint's Data Breach.

138. He is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Bone & Joint's Data Breach.

139. He suffered actual injury from the exposure and theft of his Private Information.

140. He has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession—is protected and safeguarded from additional breaches.

141. Had he been aware that Bone & Joint's computer systems were not secure, he would not have entrusted Bone & Joint with his PII and PHI.

Plaintiff Christopher VanGoethem

142. Plaintiff Christopher VanGoethem is and at all times mentioned herein was an individual citizen residing in the State of Wisconsin.

143. He is a former patient of Defendant—having received services between July 2022 and January 2023. As a condition of receiving medical services, he provided Defendant with his Private Information. Defendant then used that Private Information to facilitate its provision of services and/or to collect payment.

144. He received a Notice of Data Breach Letter related to Bone & Joint's Data Breach that is dated March 7, 2023. *See* Exhibit A.

145. The Notice Letter does not explain exactly which parts of his PII and PHI were accessed and taken but instead generically states that the files contained his "name, date of birth, Social Security number, home address, phone number, health insurance information, and diagnosis and treatment information." *See* Ex. A.

146. He is especially concerned that his Private Information was stolen and that his Social Security number was identified as among the breached data on Bone & Joint's computer system.

147. He does not recall ever learning that his Private Information had ever been compromised in a data breach incident other than the breach at issue here.

148. Moreover, Plaintiff has experienced significant identity theft and fraud because of Defendant's Data Breach. In March 2023, Plaintiff received an email from Venmo stating that his password had been changed and, subsequently two fraudulent transactions were made. Also in March 2023, an unidentified person went to two separate AT&T stores in Lakewood, Florida with a copy of Plaintiffs' driver's license and Social Security Number and opened two new telephone

lines, closed Plaintiff's wife's telephone line, and purchased $5,000 worth of products. Then, in April 2023, a loan for $2,500 was taken in Plaintiff's name. These incidents clearly show that Plaintiff's Private Information stolen in the Data Breach is in the hands of cybercriminals.

149. Since experiencing those instances of fraud, Plaintiff has locked all his accounts and created fraud alerts for each.

150. Plaintiff has spent—and will continue to spend—significant time and effort diligently monitoring his accounts to protect himself from identity theft. Defendant directed Plaintiff to take those steps in its breach notice. Plaintiff fears for his personal financial security.

151. He is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Bone & Joint's Data Breach.

152. He suffered actual injury from the exposure and theft of his Private Information.

153. He has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession—is protected and safeguarded from additional breaches.

154. Had he been aware that Bone & Joint's computer systems were not secure, he would not have entrusted Bone & Joint with his PII and PHI.

Plaintiff Kal Tesky

155. Plaintiff Kal Tesky is and at all times mentioned herein was an individual citizen residing in the State of Wisconsin.

156. He is a former patient of Defendant—having provided Defendant with his Private Information and received medical services from Defendant. Defendant then used that Private Information to facilitate its provision of services and/or to collect payment.

157. Upon information and belief, he received a Notice of Data Breach Letter, related to Bone & Joint's Data Breach that is dated March 7, 2023.

158. He has always is very careful about sharing his Private Information. He has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

159. He stores any documents containing his Private Information in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts. Had he known Defendants failed to follow basic industry security standards and failed to implement systems to protect his Private Information, he would not have provided that information to Defendant.

160. In light of the Data Breach, he is especially concerned that his Private Information was stolen and that his Social Security number was identified as among the breached data on Bone & Joint's computer system.

161. Upon information and belief, because of Defendant's Data Breach, in April 2023, he experienced fraudulent attempts to transfer $150 from his PayPal account. Although the attempts were stopped by Plaintiff and PayPal, it demonstrates that the Private Information stolen in the Data Breach is in the hands of cybercriminals.

162. As a result of the Data Breach, he heeded Defendant's warning and spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendants advised him to mitigate his damages by, among other things, monitoring

his accounts for fraudulent activity. Plaintiff has spent—and will continue to spend—significant time and effort diligently monitoring his accounts to protect himself from identity theft.

163. He is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Bone & Joint's Data Breach.

164. He suffered actual injury from the exposure and theft of his Private Information.

165. He has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession—is protected and safeguarded from additional breaches.

166. Had he been aware that Bone & Joint's computer systems were not secure, he would not have entrusted Bone & Joint with his PII and PHI.

COMMON INJURIES AND DAMAGES

167. As result of Defendant's ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

168. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including but not limited to: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in

Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

The Risk of Identity Theft to Plaintiffs and Class Members is Present and Ongoing

169. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

170. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

171. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

172. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[40] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[41] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

173. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII and PHI at issue here.[42] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[43] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[44]

---

[40] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[41] *Id.*

[42] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

[43] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[44] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

174. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[45]

175. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

176. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[46]

---

[45] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[46] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

177. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[47]

178. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[48]

179. One such example of criminals using PHI for profit is the development of "Fullz" packages. Cyber-criminals can cross-reference two sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

180. The development of "Fullz" packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain

[47] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[48] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and Class Members' stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

181. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[49]

182. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[50] Defendant did not rapidly report to Plaintiffs and the Class that their Private Information had been stolen.

183. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

184. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute

[49] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

[50] *Id.*

charges with creditors.

185. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PHI. To protect themselves, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

186. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[51]

187. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[52]

---

[51] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

[52] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

188. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[53]

189. Defendant's failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

190. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

191. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant's Notice instructs them, "remain vigilant against incidents of identity theft and fraud by reviewing [their] account statements, explanation of benefits, and free credit reports for unexpected activity or errors over the next 12 to 24 months."

---

[53] *See, e.g.*, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices.

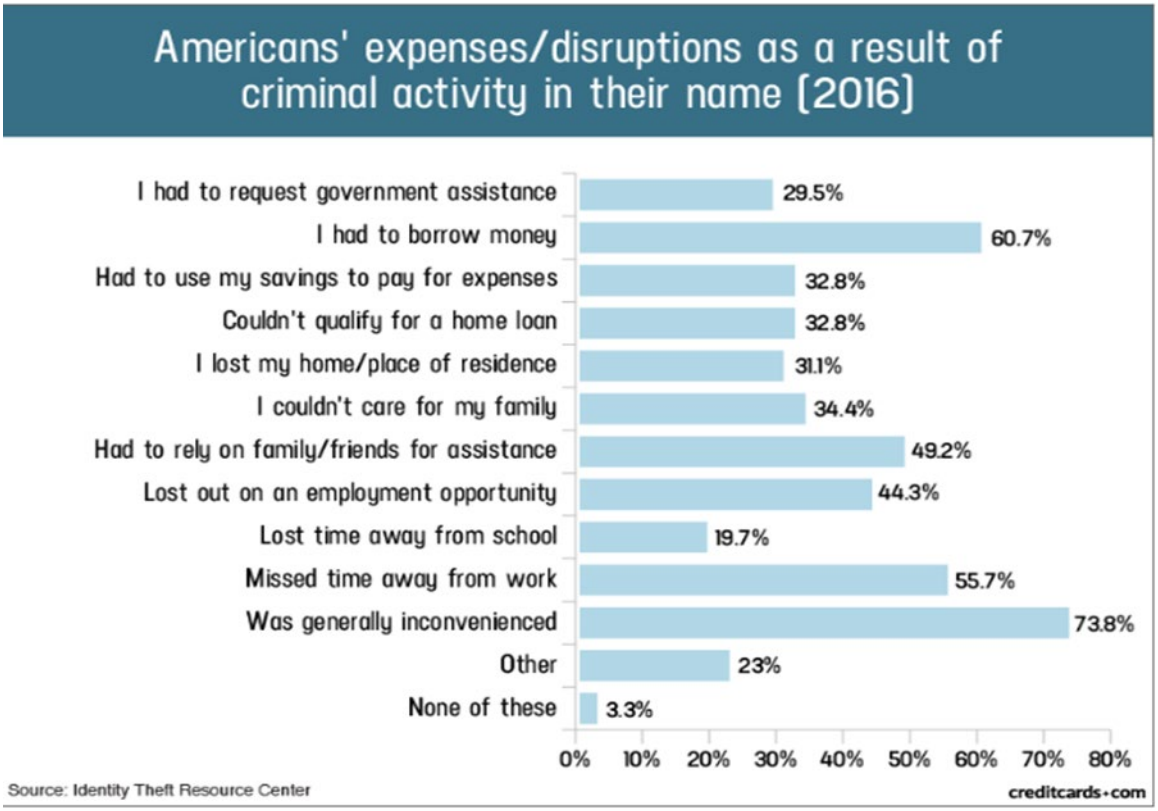
192. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

193. Plaintiffs' mitigation efforts are consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[54]

194. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[55]

[54] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps.

[55] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



195. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[56] Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from

[56] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

their accounts, placing a credit freeze on their credit, and correcting their credit reports.[57]

Diminution of Value of the Private Information

196. PII/PHI is a valuable property right.[58] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

197. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

198. Private Information can sell for as much as $363 per record according to the Infosec Institute.[59]

199. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data was selling on the dark web for $50 and up.[60]

200. An active and robust legitimate marketplace for Private Information also exists. In

---

[57] *See* https://www.identitytheft.gov/Steps.

[58] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[59] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[60] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

2019, the data brokering industry was worth roughly $200 billion.[61] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[62, 63] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[64]

201. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

202. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach – Defendant has only offered 12 months of inadequate identity monitoring services through IDX, despite Plaintiffs and Class Members being at risk of identity theft and fraud for the foreseeable future. Defendant has not offered any other relief or protection. Furthermore, this is a tacit admission that its failure to protect their Private Information has caused Plaintiffs and Class great injuries. See Ex. A.

203. Defendant also places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

---

[61] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[62] https://datacoup.com/.

[63] https://digi.me/what-is-digime/.

[64] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

204. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

205. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

206. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[65] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

207. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

208. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members

[65] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss of Benefit of the Bargain

209. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to provide their Private Information, which was a condition precedent to employment or to obtain services, and paying Defendant for its services, Plaintiffs as reasonable employees and consumers understood and expected that they were, in part, paying, or being paid less, for services and data security to protect the Private Information required to be collected from them.

210. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Injunctive Relief is Necessary to Protect Against Future Data Breaches

211. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

212. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

Lack of Compensation

213. Bone & Joint's credit monitoring offer fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

214. Plaintiffs and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

215. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and

identity theft.

216. Further, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

217. Specifically, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing “freezes” and “alerts” with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic

payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

218. In addition, Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the property of loss of value damages in related cases.

219. Plaintiffs and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

220. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII and PHI. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Bone & Joint knew of the breach since January 16, 2023 and waited nearly 2 months to notify them. They have yet to offer an explanation of purpose for the delay. This delay violates HIPAA and other notification requirements and increases the injuries to Plaintiff(s) and Class.

CLASS ACTION ALLEGATIONS

221. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

222. The Nationwide Class that Plaintiffs seeks to represent is defined as follows:

> All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach for which Defendant

> Bone & Joint provided notice to Plaintiffs and other Class Members beginning on or around March 7, 2023 (the "Class").

223. In addition, Plaintiffs seek to represent a Wisconsin subclass, defined as follows:

> All persons who are citizens of Wisconsin whose Private Information was actually or potentially accessed or acquired during the Data Breach for which Defendant Bone & Joint provided notice to Plaintiffs and other Class Members beginning on or around March 7, 2023 (the "Wisconsin Subclass") (collectively, the "Classes").

224. Excluded from the Class(es) are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

225. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

226. Numerosity, Fed. R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are in excess of 105,094 individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.[66]

227. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

---

[66] Breach Portal, U.S. Dept. of Health and Hum. Servs., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited May 3, 2023).

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

228. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

229. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

230. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs has suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

231. Superiority, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for

those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

232. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

233. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, including its privacy policy, uniform methods of data collection, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

234. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

235. Unless a classwide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Consolidated Amended Complaint.

236. Further, Defendant has acted or refused to act on grounds generally applicable to

the Classes and, accordingly, class certification, injunctive relief, and corresponding declaratory relief are appropriate on a classwide basis.

237. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members; and

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and All Class Members)

238. Plaintiffs and the Class repeat and re-allege each and every allegation in the Consolidated Amended Complaint as if fully set forth herein.

239. Defendant required Plaintiffs and Class Members to submit non-public personal information in order to obtain healthcare services.

240. Defendant owed a duty of care to secure and safeguard the computer systems holding Plaintiffs' and Class Members' Private Information that Defendant acquired.

241. The duty included obligations to take reasonable steps to prevent disclosure of the Private Information, and to safeguard the information from theft. Defendant's duties included the responsibility to design, implement, and monitor data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

242. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the Private Information.

243. Defendant owed a duty of care to safeguard the Private Information due to the foreseeable risk of a data breach and the severe consequences that would result from its failure to so safeguard the Private Information.

244. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its employees and its patients, which is recognized by laws and regulations, including but not limited to HIPAA and the FTC Act, as

well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

245. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

246. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

247. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information that it either acquires, maintains, or stores.

248. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information, as alleged and discussed above.

249. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

250. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

251. The imposition of a duty of care on Defendant to safeguard the Private Information they maintained is appropriate because any social utility of Defendant's conduct is outweighed by the injuries suffered by Plaintiffs and Class Members as a result of the Data Breach.

252. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

253. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

254. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

255. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to

future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and All Class Members)

256. Plaintiffs and the Class repeat and re-allege each and every allegation in the Consolidated Amended Complaint as if fully set forth herein.

257. Pursuant to Federal Trade Commission, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

258. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

259. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

260. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

261. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

262. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

263. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

264. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

265. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

266. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and All Class Members)

267. Plaintiffs and the Class repeat and re-allege each and every allegation in the Consolidated Amended Complaint as if fully set forth herein.

268. Plaintiffs and the Class entrusted their Private Information to Defendant. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

269. In its Privacy Policy, Bone & Joint represented that it would not disclose Plaintiffs' and Class Members' Private Information to unauthorized third-parties.

270. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

271. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information and to destroy any Private Information that it was no longer required to maintain.

272. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

273. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices.

274. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

275. In accepting the Private Information of Plaintiffs and Class Members, Defendant understood and agreed that they were required to reasonably safeguard the Private Information from unauthorized access or disclosure.

276. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, the FTC Act, and were consistent with industry standards.

277. Plaintiffs and Class Members agreed to employment and/or paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

278. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their Private Information reasonably secure.

279. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

280. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

281. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information or to destroy it once it was no longer necessary or able to retain the Private Information.

282. As a direct and proximate result of Defendant's breach of the implied promises, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained incidental and consequential damages including: (a) financial "out of

pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) financial "out of pocket" costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) diminution of value of their Private Information; (g) future costs of identity theft monitoring; (h) and the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

283. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

284. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and All Class Members)

285. Plaintiffs and the Class repeat and re-allege each and every allegation in the Consolidated Amended Complaint as if fully set forth herein.

286. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendants became guardians of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff s and Class Members, (1) for the safeguarding of

Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and do store.

287. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with its patients, in particular, to keep secure their Private Information.

288. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

289. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

290. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

291. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

292. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members sustained compensatory damages including (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity

theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

293. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

294. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT V
INVASION OF PRIVACY (Violations of Wis. Stat. § 995.50 *et seq.*)
(On Behalf of Plaintiffs and the Subclass)

295. Plaintiffs and the Class repeat and re-allege each and every allegation in the Consolidated Amended Complaint as if fully set forth herein.

296. The State of Wisconsin recognizes the right of privacy as codified by Wis. Stat. § 995.50 *et seq.*

297. As relevant here, Wisconsin statutes define invasion of privacy" as the following:

a. "Intrusion upon the privacy of another of a nature highly offensive to a reasonable person . . ., in a place that a reasonable person would consider private, or in a manner that is actionable for trespass."[67]

b. "Publicity given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person, if the defendant has acted either unreasonably or recklessly

[67] Wis. Stat. § 995.50(2).

as to whether there was a legitimate public interest in the matter involved, or with actual knowledge that none existed."[68]

298. Moreover, Wisconsin statute declares that this right of privacy "shall be interpreted in accordance with the developing common law of privacy."[69]

299. Plaintiffs and the Class had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to its protection against disclosure to unauthorized third parties.

300. Defendant owed a duty to its patients, including Plaintiffs and the Class, to keep this Private Information confidential.

301. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class members' Private Information is highly offensive to a reasonable person.

302. The intrusion was into a place or thing (victim's place of business or medical services) which was private and entitled to be private. Plaintiffs and the Class were required disclose their Private Information to Defendant to further their employment or obtain medical services with the intention that it would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

303. The Data Breach constitutes an intentional interference with Plaintiffs and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

---

[68] *Id*.

[69] Wis. Stat. § 995.50(3).

304. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

305. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

306. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

307. As a proximate result of Defendant's acts and omissions, the Private Information of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages as detailed herein.

308. Under Wisconsin law, those whose privacy is unreasonably invaded—such as Plaintiffs and Class Members—are entitled to the following types of relief:

a. "Equitable relief to prevent and restrain such invasion, excluding prior restraint against constitutionally protected communication privately and through the public media;"[70]

b. "Compensatory damages based either on plaintiff's loss or defendant's unjust enrichment;"[71] and

c. "A reasonable amount for attorney fees."[72]

[70] Wis. Stat. § 995.50(1).

[71] *Id*.

[72] *Id*.

309. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information is still maintained by Defendant with its inadequate cybersecurity system and policies.

310. Plaintiffs and the Class have no adequate remedy at law for the ongoing injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiffs and the Class.

311. Plaintiffs, on behalf of themselves and other Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT VI
UNFAIR AND DECEPTIVE BUSINESS PRACTICES
(Violations of § 134.98, WIS. STAT. and § 100.18, WIS. STAT.)
(On Behalf of Plaintiffs and the Subclass)

312. Plaintiffs and the Class repeat and re-allege each and every allegation in the Consolidated Amended Complaint as if fully set forth herein.

313. This is a claim for violation of §134.98, Wis. Stat.

314. § 100.18, Wis. Stat. provides that unfair methods of competition, unconscionable acts and practices, and unfair or deceptive acts or practices in the conduct "of any trade or commerce" are unlawful.

315. Plaintiffs and Class Members are "persons" as defined and construed under § 134.98, Wis. Stat. and § 100.18, Wis. Stat.

316. Defendant's conduct as alleged herein occurred in the course of trade or commerce.

317. Defendant's failure to maintain reasonable procedures designed to protect against unauthorized access while transferring and/or maintaining possession of the Private Information constitutes an unfair or deceptive trade practice, as do the following violations:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures in response to increasing cybersecurity risks in the healthcare sector, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501–6505, as well as its own policies, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII and PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501–6505;

f. Failing to timely and adequately notify Plaintiffs and Class Members of the Data Breach;

g. Misrepresenting that certain Private Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with the common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501–6505, and did not comply with its own policies.

318. Further, Defendant's failure to properly give notice of the breach of the security of the computerized data system pursuant to § 134.98, Wis. Stat. constitutes an unfair or deceptive practice.

319. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Class Members, about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

320. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Class Members, leading them to believe for a prolonged period of time that their Private Information was secure and that they did not need to take actions to secure their identities.

321. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

322. Had Defendant disclosed to Plaintiffs and Class Members that its network systems were not secure and thus vulnerable to attack, Defendant would have been forced to adopt reasonable data security measures and comply with the law. Instead, Plaintiffs and Class Members entrusted Defendant with their sensitive and valuable Private Information. Defendant accepted the responsibility of being a steward of this data, while keeping the inadequacy of its security measures secret from the public. Accordingly, because Defendant held itself out as maintaining a secure system for such data, Plaintiffs and Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

323. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices and Plaintiffs' and Class Members' reliance on them, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring financial accounts for fraudulent activity; imminent risk of fraud and identity theft; loss of privacy; loss of value of their Private Information and other economic and non-economic harm and relief the Court deems necessary or proper.

COUNT VII
CONFIDENTIALITY OF PATIENT HEALTH CARE RECORDS
(Violations of Wis. Stat. §§ 146.82, 146.84)
(On Behalf of Plaintiffs and the Subclass)

324. Plaintiffs and the Class repeat and re-allege each and every allegation in the Consolidated Amended Complaint as if fully set forth herein.

325. Wisconsin law prohibits the unauthorized release of health care information. Specifically, Wis. Stat. § 146.82(1) requires that "All patient health care records shall *remain confidential*. Patient health care records may be released only to the persons designated in this

section or to other persons with the *informed consent* of the patient or of a person authorized by the patient."

326. In turn, such statutory violations of are afforded a private cause of action under Wis. Stat. § 146.84(1). Specifically, Wis. Stat. § 146.84(1) states that:

a. "Any person, including the state or any political subdivision of the state, who *negligently violates* s. 146.82 or 146.83 shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than $1,000 and costs and reasonable actual attorney fees;" and

b. "An individual may bring an action to enjoin any violation of s. 146.82 or 146.83 or to compel compliance with s. 146.82 or 146.83 and may, in the same action, seek damages as provided in this subsection."

327. Moreover, Wis. Stat. § 146.84(2) mandates that these statutory violations are subject to the following penalties: "[w]hoever *negligently* discloses confidential information in violation of s. 146.82 is subject to a forfeiture of not more than $1,000 for each violation."

328. Defendant violated Wis. Stat. § 146.84(1) by failing to keep patient records confidential. Instead, through its negligent data security practices, Defendant exposed patients' health care records to third parties without patients' informed consent or authorization. Thus, Defendant is liable to Plaintiffs and Class Members for actual damages. exemplary damages, and costs and reasonable actual attorney fees.

329. Additionally, Plaintiffs seeks an injunction to enjoin Defendant from its practice of disclosing patient health records and to compel Defendant's compliance with Wis. Stat. § 146.82.

COUNT VIII
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and All Class Members)

330. Plaintiffs and the Class repeat and re-allege each and every allegation in the Consolidated Amended Complaint as if fully set forth herein.

331. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information. Indeed, in acquiring the Private Information, Defendant was then able to employ skilled workers and charge money for its medical services.

332. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information, which cost savings increased the profitability of the services.

333. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

334. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

335. Defendant acquired the monetary benefit of the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

336. Had Plaintiffs and Class Members known that Defendant had not secured their

Private Information, they would not have agreed to provide it to Defendant. Plaintiffs and Class Members have no adequate remedy at law.

337. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

338. Furthermore, as a direct and proximate result of Defendant's unreasonable and inadequate data security practices, Plaintiffs and Class Members are at a current and ongoing risk of identity theft and have sustained incidental and consequential damages, including: (a) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) financial "out of pocket" costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; and (i) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

339. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

340. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

341. Moreover, Defendant should be compelled to disgorge into a common fund or

constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT IX
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and All Class Members)

342. Plaintiffs and the Class repeat and re-allege each and every allegation in the Consolidated Amended Complaint as if fully set forth herein.

343. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

344. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

345. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

346. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect employee and patient Private Information.

347. Defendant still possesses the Private Information of Plaintiffs and the Class.

348. To Plaintiffs' knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

349. To Plaintiffs' knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

350. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Bone & Joint. The risk of another such breach is real, immediate, and substantial.

351. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

352. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

353. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Bone & Joint, Plaintiffs and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

354. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Bone & Joint, thus eliminating the additional injuries that would result to Plaintiffs and the Class.

355. Plaintiffs and Class Members therefore, seek a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

e. Ordering that Defendant conduct regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, client personally identifiable information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, and appointing Plaintiffs and their Counsel to represent the Class;

B. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

C. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

D. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information

Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information as well as protecting the Private Information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and

education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting Private Information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the

Court's final judgment;

E. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: May 22, 2023

Respectfully Submitted,

/s/ *Lisa A. White*
Lisa A. White (admitted, WD of Wisconsin)
Gary E. Mason*
Danielle L. Perry*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290
lwhite@masonllp.com
gmason@masonllp.com
dperry@masonllp.com

/s/ *Ken Grunfeld*
KENNETH J. GRUNFELD (admitted, WD of Wisconsin)
KEVIN FAY*
GOLOMB SPIRT GRUNFELD P.C.
1835 Market Street, Suite 2900
Philadelphia, Pennsylvania 19103
Telephone: (215) 346-7338
Facsimile: (215) 985-4169
KGrunfeld@GolombLegal.Com
Kfay@GolombLegal.Com

Samuel J. Strauss (Bar No. 1113942)
Raina C. Borrelli
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone: 608-237-1775
Facsimile: 608-509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Joseph M. Lyon*
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Counsel for Plaintiffs and Putative Class

* *Pro hac vice* pending